MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

| DOMANDA DI INVENZIONE NUMERO | 102021000020696 |
|---|---|
| Data Deposito | 02/08/2021 |
| Data Pubblicazione | 02/02/2023 |

Classifiche IPC

| Sezione | Classe | Sottoclasse | Gruppo | Sottogruppo |
|---|---|---|---|---|
| G | 06 | F | 21 | 64 |

| Sezione | Classe | Sottoclasse | Gruppo | Sottogruppo |
|---|---|---|---|---|
| G | 06 | F | 21 | 62 |

| Sezione | Classe | Sottoclasse | Gruppo | Sottogruppo |
|---|---|---|---|---|
| G | 06 | F | 21 | 36 |

| Sezione | Classe | Sottoclasse | Gruppo | Sottogruppo |
|---|---|---|---|---|
| H | 04 | L | 9 | 32 |

Titolo

METODO E SISTEMA PER LA VERIFICA SICURA DI UN TITOLO

# METODO E SISTEMA PER LA VERIFICA SICURA DI UN TITOLO

* * *

## CAMPO TECNICO

La presente invenzione si riferisce al settore dei sistemi informatici. In dettaglio, la presente invenzione riguarda un metodo e un sistema per la verifica sicura di un titolo, laddove con "titolo" si intende un biglietto per un evento (a titolo esemplificativo, ma non esaustivo, di tipo musicale, artistico, culturale, cinematografico, teatrale, fieristico, di intrattenimento ricreativo, ludico e formativo), in presenza o in remoto (per esempio, in diretta streaming o in differita), un biglietto per mezzi di trasporto, certificati ufficiali, documenti di identità, un biglietto aventi ad oggetto una transazione, contratto e attività prodromiche e successive alla conclusione degli stessi, nonché il compimento di attività nell'area scientifica, tecnica, filatelica, numismatica e collezionistica, sportiva, artistica, della moda, giuridica e bancaria in genere,.

## STATO DELL'ARTE

La diffusione capillare di sistemi informatici collegati tra loro per mezzo della rete internet, così come la diffusione di smartphone e simili dispositivi elettronici ha portato a una rapida e pervasiva diffusione di sistemi digitali e servizi per acquisti, finanziari, ecc.

Tuttavia, la relativa semplicità di riproduzione di dati digitali pone un serio problema alla possibilità di identificare e autenticare individui o documenti, in quanto dati privati e documenti possono essere replicati virtualmente all'infinito con uno sforzo minimo.

Nel tentativo di risolvere tale problema, nella tecnica sono state proposte svariate soluzioni, molte delle quali si basano sull'identificazione di utenti o sulla limitazione dell'accesso a dati digitali sensibili attraverso uno o più fattori di autenticazione come password, codici temporanei e/o dati biometrici.

In particolare, nel caso di titoli digitali questi accorgimenti non sono applicabili o hanno un'efficacia molto limitata. Infatti, i titoli in formato digitale, per esempio biglietti aerei e di altri mezzi di trasporto, solitamente includono un codice identificativo univoco assegnato al momento della generazione del titolo.

Tuttavia, è noto che una semplice immagine del codice identificativo, per esempio diffusa inavvertitamente dal legittimo proprietario, consenta a individui competenti di riutilizzare indebitamente il codice univoco, e il titolo associato, e/o

accedere a informazioni riservate relative al proprietario e/o al distributore del titolo.

**SCOPI E RIASSUNTO DELL'INVENZIONE**

Compito della presente invenzione è quello di superare gli inconvenienti dell'arte nota. In particolare, nell'ambito di tale compito, è scopo della presente invenzione fornire un metodo e un relativo sistema in grado di eseguire una rapida e sicura verifica di un titolo.

Ulteriore scopo della presente invenzione è di fornire un metodo e un relativo sistema che permetta la gestione di titoli digitali in modo completamente automatico o con un intervento marginale da parte di operatori umani.

Il compito sopra esposto, nonché gli scopi della presente invenzione sono raggiunti mediante un metodo per la verifica sicura di un titolo in un metodo secondo l'allegata rivendicazione 1 e un sistema per la verifica sicura di un titolo secondo l'allegata rivendicazione 10.

Ulteriori caratteristiche delle forme di realizzazione preferite del metodo per la verifica sicura di un titolo secondo la presente invenzione sono oggetto delle rivendicazioni dipendenti.

**BREVE DESCRIZIONE DEI DISEGNI**

Ulteriori caratteristiche e vantaggi della presente invenzione risulteranno meglio dalla seguente descrizione dettagliata di alcune sue forme di realizzazione preferite, ma non esclusive, fatta con riferimento ai disegni allegati.

In tali disegni,

- la figura 1 è uno schema a blocchi di un sistema secondo una forma di realizzazione della presente invenzione;
- la figura 2 è un diagramma di flusso di una procedura di creazione di NFT secondo una forma di realizzazione della presente invenzione;
- la figura 3 è uno schema a blocchi che illustra alcuni passi della procedura di figura 2;
- la figura 4 è un diagramma di flusso di una procedura di assegnazione di NFT secondo una forma di realizzazione della presente invenzione;
- la figura 5 è uno schema a blocchi di una porzione di registro digitale distribuito in cui sono registrate transazioni durante l'esecuzione della procedura di figura 4;

- la figura 6 è un diagramma di flusso di una procedura per la verifica sicura dei titoli secondo una forma di realizzazione della presente invenzione;

- la figura 7 è uno schema a blocchi che mostra lo scambio di un codice di verifica tra elementi del sistema di figura 1 effettuato durante l'esecuzione della procedura di figura 6, e

- la figura 8 è un diagramma di flusso di una procedura di creazione di NFT secondo una forma di realizzazione alternativa della presente invenzione.

**DESCRIZIONE DETTAGLIATA DELL'INVENZIONE**

Nella seguente descrizione, per l'illustrazione delle figure si ricorre a numeri o simboli di riferimento identici per indicare elementi costruttivi con la stessa funzione. Inoltre, per chiarezza di illustrazione, alcuni riferimenti possono non essere ripetuti in tutte le figure.

Mentre l'invenzione è suscettibile di varie modifiche e costruzioni alternative, alcune forme di realizzazione preferite sono mostrate nei disegni e saranno descritte qui di seguito in dettaglio. Si deve intendere, comunque, che non vi è alcuna intenzione di limitare l'invenzione alla specifica forma di realizzazione illustrata, ma, al contrario, l'invenzione intende coprire tutte le modifiche, costruzioni alternative ed equivalenti che ricadano nell'ambito dell'invenzione come definito nelle rivendicazioni.

L'uso di "a esempio", "ecc.", "oppure" indica alternative non esclusive senza limitazione a meno che non altrimenti indicato. L'uso di "comprende" e "include" significa "comprende o include, ma non limitato a" a meno che non altrimenti indicato.

Con riferimento alla figura 1, è illustrata una forma di realizzazione preferita di un sistema informatico secondo la presente invenzione, nel seguito semplicemente il sistema 1, che comprende una prima entità remota di elaborazione, per esempio un server 10, un apparato lettore 20, un dispositivo utente 30, un registro digitale distribuito 40 e una rete di archiviazione dati 50.

Nell'esempio considerato, il server 10 comprende un modulo elaborare 11 – per esempio formato da uno o più processori, unità di memoria volatile e non-volatile, acceleratori grafici, ASIC, ecc. –, un modulo di archiviazione 12 configurato per archiviare grandi quantità di dati, per esempio in un database e un modulo di comunicazione 13 configurato per scambiare dati attraverso un canale di comunicazione dati – per esempio un modem.

L'apparato lettore 20 è configurato per acquisire elaborare e trasmettere attraverso un canale di comunicazione dati immagini digitali. A tale scopo, l'apparato lettore 20 comprende una fotocamera 21, un modulo elaboratore 22 e un modulo di comunicazione 23.

Il dispositivo utente 30 è configurato per elaborare e scambiare dati attraverso un canale di comunicazione dati e visualizzare informazioni in formato grafico. A tale scopo, il dispositivo utente 30 comprende un modulo elaboratore 31, un modulo di comunicazione 32 e uno schermo 33. Esempi di dispositivo utente 30 comprendono, in modo non limitativo, smartphone, dispositivi elettronici indossabili (anche noti con il termine inglese *wearables*) e tablet.

Il registro digitale distribuito 40 è configurato per conservare dati digitali cifrati in modo inalterabile. A tale scopo, il registro digitale distribuito 40 comprende una pluralità di blocchi dati B0-Bn organizzati in una serie o catena inalterabile formata secondo i criteri della tecnologia dei registri distribuiti o *Distributed Ledger Technology* (DLT). Il registro digitale distribuito 40 è mantenuto da una rete di elaboratori elettronici – rappresentati schematicamente da una nuvola 60 in Figura 1 – di tipo da pari a pari. Per esempio, Il registro digitale distribuito 40 comprende un registro tra Bitcoin, Ethereum, Algoran o simili.

Preferibilmente il sistema 1 comprende – o è connesso a - una rete di dispositivi elettronici per l'archiviazione di dati in modo distribuito, chiamata rete di archiviazione dati 50 nel seguito. Nell'esempio considerato, la rete di archiviazione dati 50 è una rete di tipo da pari a pari, o peer to peer – P2P. Per esempio, la rete di archiviazione dati 50 comprende il file di sistema interplanetario o IPFS (InterPlanetaty File System).

Il sistema 1 appena descritto consente di implementare un metodo per verificare un modo sicuro un titolo – per esempio un biglietto per un evento di intrattenimento (come un evento sportivo, musicale, teatrale, ecc.) – secondo una forma di realizzazione della presente invenzione. Nell'esempio considerato, la distribuzione dei biglietti per l'evento intrattenitore è gestita da una terza parte, un venditore di biglietti nell'esempio considerato, la quale controlla un apparato di distribuzione 70 – per esempio, un altro server, un sistema di biglietteria virtuale, ecc. – configurato per scambiare dati con il server 10.

Il metodo comprende una procedura 100 di creazione di NFT, di cui la figura 2 rappresenta un diagramma di flusso e la figura 3 uno schema a blocchi.

La procedura 100 è avviata quando è ricevuta una richiesta di generazione *req*

di uno o più token crittografici non fungibili o *Non-Fungible Token* (NFT) al server 10 (blocco 101). La richiesta di generazione *req* di NFT comprende informazioni venditore che permettono di identificare un venditore di titoli da associare allo NFT. Per esempio, la richiesta di generazione *req* di NFT è inoltrata dall'apparato di distribuzione 70 del venditore.

Nell'esempio considerato, la richiesta di generazione *req* di NFT comprende, inoltre, un contenuto digitale D da associare agli NFT. Per esempio, il contenuto digitale D comprende un file contenente un'immagine bidimensionale o tridimensionale, una sequenza di immagini, un filmato, una registrazione acustica, ecc. – come l'immagine di un biglietto dell'evento di intrattenimento.

Il server 10 registra il contenuto digitale D nella rete di archiviazione dati 50 e acquisisce un indirizzo $H_{IPFS}$ del contenuto digitale D all'interno della rete di archiviazione dati 50 (blocco 103), per esempio un hash univoco usato per identificare il contenuto digitale D all'interno della rete di archiviazione dati 50.

Successivamente, il server 10 genera almeno un NFT associato al contenuto digitale D (blocco 103). Per esempio, il server 10 inoltra al registro digitale distribuito 40 una richiesta di creazione di un NFT N secondo lo Standard ERC-721 o ERC-1155.

In generale, lo NFT N è un insieme di dati relativi al contenuto digitale D, ossia l'immagine del biglietto, e/o a un bene materiale/immateriale associato, la possibilità di avere accesso all'evento di intrattenimento. Vantaggiosamente, lo NFT comprende, in modo non limitativo:

- l'indirizzo del contenuto $H_{IPFS}$ del contenuto digitale D all'interno della rete di archiviazione dati 50,
- metadati relativi al contenuto digitale D o un collegamento a un file (tipicamente un file .json) contenente metadati relativi al contenuto digitale D,
- un rispettivo codice di Hash $H_{NFT}$, e
- un codice di identificazione $ID_{NFT}$.

In particolare, lo NFT N non è reciprocamente intercambiabile con un altro NFT anche se generato dallo stesso algoritmo.

Lo NFT N rappresenta quindi una prova di acquisto o possesso di un titolo – un biglietto per l'evento di intrattenimento nell'esempio considerato – unico e non confondibile con uno altro NFT e il corrispondente titolo.

Lo NFT N è, preferibilmente associato a un identificatore venditore IDF associato al venditore corrispondente (blocco 105). Per esempio, l'identificatore venditore

IDF è una chiave pubblica di un cosiddetto *wallet* per criptovalute o l'indirizzo di un *data locker* associato al venditore. Preferibilmente, il server 10 mantiene un database relazionale cifrato archiviato nel modulo di archiviazione 12 del server 10 comprendente una lista di identificatori venditore IDF. Vantaggiosamente, l'identificatore venditore IDF è una chiave pubblica di un cosiddetto *wallet* per criptovalute o l'indirizzo di un *data locker* associato all'utente, eventualmente creato o allocato ad-hoc per il venditore se non presente nel database relazionale cifrato.

In particolare, contestualmente alla generazione dello NFT N, è creato un contratto intelligente o smart contract SC il quale è registrato in un blocco Bn del registro digitale distribuito 40, il quale è identificato da un corrispondente codice di hash $H_{SC}$. In particolare, lo smart contract SC comprende un codice software che permette di gestire automaticamente il cambio di proprietà dello NFT N attraverso transazioni registrate nel registro digitale distribuito 40 e una pluralità di dati associati allo NFT.

In generale, la pluralità di dati comprende:

- l'identificatore del venditore IDF
- informazioni sullo NFT, tra cui
  - un rispettivo codice di Hash $H_{NFT}$,
  - un codice di identificazione $ID_{NFT}$,
  - l'indirizzo del contenuto $H_{IPFS}$, e
- Metadati relativi allo smart contract SC.

Il sistema 1 implementa una procedura 200 di distribuzione degli NFT N agli utenti finali, gli acquirenti del biglietto nell'esempio, di cui la figura 4 è un diagramma di flusso e la figura 5 è uno schema a blocchi di alcuni passi rilevanti.

La procedura 200 ha inizio quando un utente effettua l'acquisto di un titolo, come il biglietto per l'evento di intrattenimento nell'esempio considerato (blocco 201). Per esempio, l'acquisto del titolo è eseguito dall'utente per mezzo di uno scambio dati tra il dispositivo utente 30 e l'apparato di distribuzione 70 del venditore. In particolare, l'acquisto del titolo è eseguito interagendo con un'interfaccia grafica di un'applicazione software eseguita dal dispositivo utente 30 collegata all'apparato di distribuzione 70 e/o collegandosi a una piattaforma online gestita dall'apparato di distribuzione 70.

L'utente che ha effettuato l'acquisto del titolo esegue una conferma del titolo, per esempio una conferma della partecipazione all'evento o dell'acquisto del titolo (blocco 203). In particolare, il generico utente utilizza il proprio dispositivo utente

30 per trasmettere un messaggio di conferma *conf*. Per esempio, l'utente fornisce una conferma della partecipazione all'evento o dell'acquisto del titolo interagendo con un'interfaccia grafica di un'applicazione software eseguita dal dispositivo utente 30 collegata all'apparato di distribuzione 70 e/o collegandosi a una piattaforma online gestita dall'apparato di distribuzione 70.

Vantaggiosamente, il messaggio di conferma *conf* comprende informazioni utente che permettono di identificare l'utente che ha acquisito il titolo. Esempi di informazioni utente comprendono, in modo non limitativo, dati anagrafici dell'utente, dati biometrici dell'utente, indirizzo MAC del dispositivo utente 30 utilizzato per un acquisto elettronico o una combinazione di tali esempi.

Di conseguenza, è selezionato un identificatore utente IDD associato all'utente corrispondente (blocco 205). Per esempio, l'apparato di distribuzione 70 trasmette almeno una delle informazioni utente ricevute al server 10. Quest'ultimo utilizza l'almeno una informazione utente per individuare il corretto identificatore utente IDD tra una pluralità di identificatori utente memorizzati in un database relazionale cifrato archiviato nel modulo di archiviazione 12 del server 10. Vantaggiosamente, l'identificatore utente IDD è una chiave pubblica di un cosiddetto *wallet* per criptovalute, eventualmente creato ad-hoc per l'utente se non presente nel database relazionale cifrato.

Il server 10 invia una richiesta di registrazione l'assegnazione dello NFT N all'utente identificato dall'identificatore utente IDD nel registro digitale distribuito 40 (blocco 207). Preferibilmente, la richiesta di registrazione comprende il codice di Hash dello NFT $H_{NFT}$, il codice di identificazione NFT $ID_{NFT}$, il codice di hash dello smart contract $H_{SC}$ e l'identificatore utente IDD. In particolare, lo smart contract SC modifica il proprietario dello NFT N associandolo all'identificatore utente IDD dell'utente che ha acquistato un corrispondente biglietto.

Una volta assegnati i titoli ai corretti utenti, il metodo comprende una procedura 300 per la verifica sicura dei titoli – di cui la figura 6 è un diagramma di flusso e la figura 7 è uno schema a blocchi di alcuni passi rilevanti.

Al momento di utilizzare il titolo, attraverso il dispositivo utente 30 è richiesto un codice di verifica CV al server 10 (blocco 301). Per esempio, l'utente trasmette una richiesta di trasmissione del codice di verifica al server 10 interagendo con l'applicazione software eseguita dal dispositivo utente 30 e/o collegandosi a una piattaforma online collegata o gestita dal server 10.

Preferibilmente, la richiesta di trasmissione comprende l'identificatore utente IDD e/o il codice di hash dello smart contract $H_{SC}$.

Il server 10, in risposta alla richiesta di trasmissione ricevuta, genera un corrispondente codice di verifica CV (blocco 303).

Nella forma di realizzazione considerata, il codice di verifica CV è calcolato in modo casuale combinando due o più dati associati o compresi allo NFT N, dati associati sul contenuto digitale D, e, eventualmente, dati associati all'utente (ossia, il possessore del titolo, il biglietto nel caso considerato).

Per esempio, il codice di verifica CV è calcolato eseguendo una combinazione non lineare casuale di almeno due, ma preferibilmente tre o più, tra i seguenti dati in ingresso:

- il codice di hash dello smart contract $H_{SC}$,
- una porzione del codice di hash dello smart contract $H_{SC}$,
- il codice di Hash dello NFT $H_{NFT}$,
- una porzione del codice di Hash dello NFT $H_{NFT}$,
- un metadato dello NFT N,
- una porzione di metadato dello NFT N,
- un metadato del contenuto digitale D (contenuto nello NFT N o nel file di metadati indicato nello NFT N),
- una porzione di un metadato del contenuto digitale D,
- una stringa alfanumerica ottenuta da una conversione del contenuto digitale D in stringa alfanumerica (attraverso un'opportuna applicazione software),
- una porzione della stringa alfanumerica ottenuta dalla conversione del contenuto digitale D,
- il codice identificatore utente IDD, e
- una porzione del codice identificatore utente IDD.

In una forma preferita della presente invenzione, il codice di verifica CV è calcolato come una combinazione casuale non-lineare dei seguenti tre elementi:

- la stringa alfanumerica ottenuta da una conversione del contenuto digitale D in stringa alfanumerica (o una sua porzione),
- il codice identificatore utente IDD (o una sua porzione), e
- il codice di hash dello smart contract $H_{SC}$ (o una sua porzione).

In altre parole, gli elementi selezionati sono utilizzati per comporre un seme di cifratura casuale fornito in ingresso a un algoritmo di cifratura che fornisce in uscita un corrispondente codice di verifica CV univoco.

La Richiedente ha determinato che questa combinazione di elementi permette di ottenere in modo rapido un codice di verifica CV univoco e sostanzialmente non

contraffabile. Infatti, la selezione di un insieme di dati cifrati certificati (o loro porzioni) permette di generare codici di verifica univoci virtualmente impossibili da prevedere o da contraffare.

In aggiunta, il server 10 calcola o seleziona un intervallo di tempo di validità $\Delta$ associato al codice di verifica CV blocco (305). Per esempio, l'intervallo di tempo di validità $\Delta$ ha una durata dell'ordine dei minuti, per esempio compreso tra 2 e 20 minuti, preferibilmente compreso tra 10 e 15 minuti, a partire da un istante di tempo di generazione del codice di verifica CV.

Il codice di verifica CV e l'intervallo di tempo di validità $\Delta$ sono trasmessi al dispositivo utente 30 che ha effettuato la richiesta (blocco 307).

Il server 10 e il dispositivo utente 30 sono configurati per rilevare il termine dell'intervallo di tempo di validità $\Delta$ fintanto che il codice di verifica non è utilizzato come descritto di seguito (blocco decisionale 309).

Se l'intervallo di tempo di validità $\Delta$ è trascorso (ramo di uscita Y del blocco 309), il codice di validità CV è invalidato (blocco 311) ed è necessario richiedere la trasmissione di un nuovo codice di validità CV'. Per esempio, il codice di validità CV è disabilitato contrassegnandolo come non valido o, più semplicemente, è cancellato dal server 10 e dal dispositivo utente 30.

Quando l'utente attraverso il dispositivo utente 30 trasmettere al server 10 una nuova richiesta di trasmissione di un codice di verifica (blocco 313) e il server 10, ricevuta la nuova richiesta di trasmissione, genera un nuovo codice di verifica CV' differente dal codice di verifica precedente (blocco 315).

In particolare, il nuovo codice di verifica CV' è calcolato tramite una combinazione lineare casuale in cui almeno uno tra:

- una porzione del codice di hash dello smart contract $H_{SC}$,
- una porzione del codice di Hash dello NFT $H_{NFT}$,
- un metadato del contenuto digitale D,
- una porzione di un metadato del contenuto digitale D,
- un metadato dello NFT N,
- una porzione di un metadato dello NFT N,
- una porzione della stringa alfanumerica ottenuta dalla conversione del contenuto digitale D,
- una porzione del codice identificatore utente IDD,e
- il criterio o algoritmo di combinazione non lineare

utilizzato per calcolare il nuovo codice di verifica CV' è differente dai dati utilizzati

in ingresso per calcolare il codice di verifica CV precedente.

Questa variazione della composizione dell'insieme di elementi selezionati per calcolare il nuovo codice di verifica CV' porta alla generazione di un nuovo seme di cifratura casuale differente da quello generato per il calcolo del precedente codice di verifica CV. Grazie a questa soluzione è possibile fornire in modo rapido ed efficiente un nuovo codice di verifica CV' sostanzialmente privo di alcuna relazione con il precedente codice di verifica CV. Di conseguenza, la possibilità di contraffare o eseguire altra frode risulta sostanzialmente annullata.

Inoltre, il server primario calcola o seleziona un nuovo intervallo di tempo di validità Δ' associato al nuovo codice di verifica (blocco 317). Opzionalmente, il nuovo intervallo di tempo di validità Δ' è differente dall'intervallo di tempo di validità Δ precedentemente calcolato.

Tornando al blocco decisionale 309, se l'intervallo di tempo di validità Δ non è concluso (ramo di uscita N del blocco 309), al momento della verifica del titolo – per esempio, all'ingresso di uno spazio in cui è tenuto l'evento di intrattenimento – il dispositivo utente 30 riceve (blocco 319) il codice di verifica CV dal server 10 e converte il codice di verifica CV in un codice a barre bidimensionale, per esempio un QR code Q (blocco 321), il quale è visualizzato (blocco 323) sullo schermo 33 del dispositivo utente 30.

Il dispositivo utente 30 è poi accostato all'apparato lettore 20 in modo che l'apparato lettore 20 acquisisca un'immagine digitale comprendente il QR code Q (blocco 325).

Il codice QR Q compreso nell'immagine digitale acquisita dall'apparato lettore 20 è decodificato per estrarre il corrispondente codice di verifica CV (blocco 327). Il codice di verifica CV è, poi, trasmesso al server 10 (blocco 329).

Il server 10 verifica la validità del codice di verifica CV estratto (blocco decisionale 331). Per esempio, il server 10 verifica una corrispondenza tra il codice CV estratto con un codice di verifica CV precedentemente trasmesso dal server 10 ed eventualmente, che il corrispondente intervallo di tempo di validità Δ non sia trascorso durante l'esecuzione dei passi descritti in relazione ai blocchi 319 - 329.

Nel caso il codice di verifica CV non sia valido (ramo di uscita N del blocco 331), il server 10 trasmette un messaggio di rifiuto *ref* al dispositivo utente 30 e/o all'apparato di lettura 20 (blocco 333). Opzionalmente, alla ricezione del messaggio di rifiuto *ref* il codice di verifica CV è cancellato dal dispositivo utente 30 e/o dal dispositivo di lettura 20. In aggiunta o in alternativa, in concomitanza al messaggio di rifiuto *ref* il server 10 mantiene bloccati – o comanda il blocco a

un apparato di controllo di – una porta o dei tornelli (non mostrati) associati all'apparato di lettura 20 (per esempio per collegamento diretto o per prossimità) che limitano l'accesso a uno spazio in cui è tenuto l'evento di intrattenimento.

Al contrario, se il codice di verifica CV è valido (ramo di uscita Y del blocco 331), il server 10 trasmette un messaggio di verifica corretta *ver* al dispositivo utente 30 ed eventualmente, all'apparato di lettura 20 (blocco 335) e, preferibilmente, marca come utilizzato il corrispondente NFT N (blocco 337). Preferibilmente, in concomitanza alla trasmissione del messaggio di verifica corretta *ver* il server 10 impedisce la generazione di un nuovo codice di verifica associato al NFT N e/o il dispositivo utente 30 disabilita la possibilità di richiedere un nuovo codice di verifica al NFT N. Come ulteriore aggiunta, in concomitanza al messaggio di verifica corretta *ver* il server 10 comanda l'apertura o lo sblocco della porta o dei tornelli di accesso allo spazio in cui è tenuto l'evento di intrattenimento associati all'apparato di lettura 20. In alternativa, la ricezione del messaggio di verifica corretta *ver* all'apparato di lettura 20 genera un segnale per un operatore che indica che l'utente possiede un titolo verificato – ossia, un biglietto valido.

Grazie al metodo sopra descritto è possibile garantire una verifica sicura e affidabile di titoli, come il biglietto considerato. In particolare, l'utilizzo di codici di verifica basati su NFT e variabili nel tempo garantisce una sostanziale immunità ai tentativi di falsificazione dei biglietti e alle frodi basate sulla copia indebita dei codici identificativi.

In aggiunta, il metodo composto dalle procedure sopra riportate permette di monitorare e controllare direttamente qualsiasi vendita secondaria di un titolo, eliminando il problema dei rivenditori non autorizzati e mercati paralleli.

È tuttavia chiaro che gli esempi sopra riportati non devono essere interpretati in senso limitativo e l'invenzione così concepita è suscettibile di numerose modifiche e varianti.

In una forma di realizzazione alternativa (non illustrata), il registro digitale distribuito che è usato per generare gli NFT è differente dal registro digitale distribuito usato per trasferire la proprietà degli NFT.

In un'altra forma di realizzazione (non illustrata), l'apparato di lettura è configurato per trasmettere direttamente l'immagine acquisita che sarà poi convertita nel corrispondente codice di verifica dal server.

In una forma di realizzazione (non illustrata), il gestore del server può corrispondere al venditore dei titoli. In questo caso, l'apparato di distribuzione dei titoli può essere compreso o implementato direttamente dal server.

Come sarà evidente al tecnico del settore, uno o più passi della medesima procedura o di differenti procedure possono essere eseguiti in parallelo tra loro o con un ordine differente da quello sopra presentato. Analogamente, uno o più passi opzionali possono essere aggiunti o rimossi da una o più delle procedure sopra descritte.

In particolare, sarà evidente che il server può essere configurato per eseguire più istanze in parallelo delle procedure sopra descritte.

In una forma di realizzazione, gli elementi selezionati per il calcolo del codice di verifica CV e/o del nuovo codice di verifica CV' sono combinati tra loro in modo casuale al fine di formare il corrispondente seme di cifratura casuale.

In una forma di realizzazione alternativa illustrata in figura 8, una procedura 400 di creazione di NFT prevede di generare una pluralità di NFT (blocco 403) in risposta a una richiesta di generazione di un gruppo di NFT da parte dell'apparato di distribuzione 70 (blocco 401). In particolare, la pluralità di NFT è associata a un medesimo evento ed è generata in modo analogo a quanto sopra descritto. La pluralità di NFT è associata al medesimo identificatore venditore IDF (blocco 405), per esempio l'indirizzo di un data locker.

Di conseguenza, quando un utente esegue l'acquisto di un biglietto la procedura 200 di assegnazione prevede di assegnare uno selezionato degli NFT della pluralità di NFT in modo analogo a quanto descritto per la procedura 200.

In questo modo è possibile ottenere preliminarmente un insieme di NFT pronti alla distribuzione. Questo permette di ridurre sensibilmente i tempi della procedura percepiti da un utente e gestire in modo semplice l'erogazione di titoli, come biglietti, a più utenti contemporaneamente.

In una forma di realizzazione alternativa (non illustrata), alla conferma del titolo è fornita la possibilità di modificare, ossia personalizzare, uno o più dati contenuti nello NFT N e/o uno o più attributi del contenuto digitale D attraverso il dispositivo utente 30.

In una forma di realizzazione alternativa (non illustrata), il sistema può essere utilizzato per eseguire acquisti esclusivi di prodotti digitali e/o tangibili, partecipare a lotterie, giochi organizzati nel contesto dell'evento di intrattenimento, per piazzare scommesse legate all'evento di intrattenimento, per abilitare connessioni a dispositivi interattivi utilizzati durante l'evento e/o particolari pagine web.

Naturalmente, tutti i dettagli sono sostituibili da altri elementi tecnicamente

equivalenti.

Per esempio, sebbene il sistema illustrato mostri un solo dispositivo utente, sarà evidente alla persona esperta che il sistema secondo la presente invenzione può comprendere una pluralità di dispositivi utente, ciascuno associato a un rispettivo utente.

Allo stesso modo, l'entità di elaborazione può essere realizzata con un singolo apparato elettronico o in modo distribuito per mezzo due o più apparati elettronici fisici e/o virtuali.

In alternativa allo IPFS, altre forme di realizzazione, prevedono che sia utilizzato un sistema di archiviazione distribuito di tipo a nuvola, o cloud, oppure un sistema di archiviazione dati privato (come il modulo di archiviazione 12 del server 10) e/o un servizio di archiviazione fornito da un datacenter di terze parti.

In forme di realizzazione alternative, anziché il codice di hash dello smart contract è utilizzato il codice hash (o una sua porzione) associato all'operazione (transazione) che assegna lo NFT all'utente per calcolare il codice di verifica.

In conclusione, i materiali impiegati, nonché le forme e le dimensioni contingenti dei dispositivi, apparati e terminali sopra menzionati potranno essere qualsiasi secondo le specifiche esigenze implementative senza per questo uscire dall'ambito di protezione delle seguenti rivendicazioni.

## RIVENDICAZIONI

1. Metodo (100; 200; 300; 400) per la verifica sicura di un titolo in un sistema informatico (1), il metodo comprendendo i passi eseguiti per mezzo di almeno un'entità di elaborazione (10) del sistema informatico (1) che consistono nel:
- generare (101 - 105; 401 - 403) un token crittografico non fungibile rappresentante un titolo,
- associare (201 - 207) il token crittografico non fungibile a uno specifico utente,
- a seguito di una richiesta ricevuta da un dispositivo utente (30), generare (303) in modo casuale un codice di verifica combinando due o più dati associati al token crittografico non fungibile,
- determinare (305) un intervallo di tempo di validità di detto codice di verifica,
- trasmettere (307) detto codice di verifica al dispositivo utente (30), e
- quando detto codice di verifica non è utilizzato per verificare il titolo entro l'intervallo di tempo di validità (309),
    - invalidare (311) detto codice di verifica, e
    - a seguito di una nuova richiesta ricevuta da detto dispositivo utente (30), generare (315) in modo casuale un ulteriore codice di verifica differente dal codice di verifica, e
    - determinare (317) un ulteriore intervallo di tempo di validità di detto ulteriore codice di verifica.

2. Metodo (100; 200; 300; 400) secondo la rivendicazione 1, ulteriormente comprendente i passi di:
- registrare (205) l'associazione tra il token crittografico non fungibile e detto utente specifico per mezzo di un contratto intelligente memorizzato in un blocco di un registro distribuito, e

in cui i passi (303, 315) di calcolare in modo casuale il codice di verifica e l'ulteriore codice di verifica comprendono di utilizzare almeno uno tra:
- un codice identificatore associato al contratto intelligente,
- una porzione del codice identificatore associato al contratto intelligente,
- un codice identificatore del token crittografico non fungibile,
- una porzione del codice identificatore del token crittografico non fungibile,
- un metadato contenuto nel token crittografico non fungibile,
- una porzione di metadato contenuto nel token crittografico non fungibile,
- un metadato di un contenuto digitale associato al token crittografico non fungibile,
- una porzione di un metadato del contenuto digitale,

- il codice identificatore utente, e
- una porzione del codice identificatore utente.

3. Metodo (100; 200; 300; 400) secondo la rivendicazione 2, in cui almeno un elemento utilizzato per calcolare il codice di verifica scelto tra:
- una porzione del codice identificatore associato al contratto intelligente,
- una porzione del codice identificatore del token crittografico non fungibile,
- una porzione di un metadato del contenuto digitale,
- un metadato contenuto nel token crittografico non fungibile,
- una porzione di un metadato contenuto nel token crittografico non fungibile,
- un metadato del contenuto digitale associato al token crittografico non fungibile,
- una porzione del codice identificatore utente, e
- un criterio o algoritmo di combinazione non lineare,

è differente da almeno un elemento utilizzato per calcolare l'ulteriore codice di verifica scelto tra:
- una porzione del codice identificatore associato al contratto intelligente,
- una porzione del codice identificatore del token crittografico non fungibile,
- una porzione di un metadato del contenuto digitale,
- un metadato contenuto nel token crittografico non fungibile,
- una porzione di un metadato contenuto nel token crittografico non fungibile,
- un metadato del contenuto digitale associato al token crittografico non fungibile,
- una porzione del codice identificatore utente, e
- un criterio o algoritmo di combinazione non lineare.

4. Metodo (100; 200; 300; 400) secondo la rivendicazione 2 o 3, in cui il token crittografico non fungibile è associato a un contenuto digitale, e in cui i passi di calcolare (303, 315) in modo casuale il codice di verifica o l'ulteriore codice di verifica, prevedono di:
- eseguire una conversione del contenuto digitale in una stringa alfanumerica, e
- utilizzare la stringa alfanumerica o una porzione della stringa alfanumerica come dato per il calcolo del codice di verifica o dell'ulteriore codice di verifica.

5. Metodo (100; 200; 300; 400) secondo la rivendicazione 2, 3 o 4, in cui i passi di calcolare (303, 315) in modo casuale il codice di verifica e l'ulteriore codice di verifica prevedono di utilizzare / generare un seme di cifratura casuale combinando, preferibilmente in modo casuale, due o più elementi selezionati tra:
- un codice identificatore associato al contratto intelligente,
- una porzione del codice identificatore associato al contratto intelligente,

- un codice identificatore del token crittografico non fungibile,
- una porzione del codice identificatore del token crittografico non fungibile,
- un metadato contenuto nel token crittografico non fungibile,
- una porzione di metadato contenuto nel token crittografico non fungibile,
- un metadato di un contenuto digitale associato al token crittografico non fungibile,
- una porzione di un metadato del contenuto digitale,
- il codice identificatore utente,
- una porzione del codice identificatore utente, e
- una stringa alfanumerica, o una porzione della stringa alfanumerica, ottenuta da una conversione in stringa alfanumerica di un contenuto digitale associato al token crittografico non fungibile.

6. Metodo (100; 200; 300; 400) secondo la rivendicazione 5, in cui generare (315) l'ulteriore codice di verifica differente dal codice di verifica prevede di utilizzare un seme di cifratura differente dal seme di cifratura utilizzato per calcolare il codice di verifica.

7. Metodo (100; 200; 300; 400) secondo una qualsiasi delle rivendicazioni precedenti, ulteriormente comprendente i passi di:
per mezzo di detto dispositivo utente:
- ricevere (319) uno tra detto codice di verifica e detto ulteriore codice di verifica,
- convertire (321) il codice di verifica ricevuto in un corrispondente codice a barre bidimensionale,
- riprodurre (323) il codice a barre bidimensionale su uno schermo del dispositivo utente, e
per mezzo di un apparato lettore (20) del sistema (1):
- acquisire (325) un'immagine del codice a barre bidimensionale riprodotto sullo schermo del dispositivo utente,
- estrarre (327) il codice di verifica ricevuto dal codice a barre bidimensionale compreso nell'immagine acquisita, e
- trasmettere (329) all'almeno un'entità di elaborazione (10) il codice di verifica ricevuto estratto dal codice a barre dimensionale, e
per mezzo dell'almeno un'entità di elaborazione (10):
- verificare (331) una corrispondenza tra il codice di verifica ricevuto estratto dal codice a barre bidimensionale e il codice di verifica generato dall'entità di elaborazione con un rispettivo intervallo di validità non trascorso,
quando detta corrispondenza è verificata, identificare (335, 337) come verificato

il titolo rappresentato dal token crittografico non fungibile.

8. Metodo (100; 200; 300; 400) secondo una qualsiasi delle rivendicazioni precedenti, in cui il passo di invalidare (311) detto codice di verifica comprende cancellare il codice di verifica al termine dell'intervallo di tempo di validità.

9. Metodo (100; 200; 300; 400) secondo la rivendicazione 7, ulteriormente comprendente il passo di impedire la generazione di un ulteriore codice di verifica una volta che il titolo rappresentato dal token crittografico non fungibile.

10. Sistema (1) per la verifica sicura di un titolo comprendente
- un'entità di elaborazione elettronica (10), e
- un dispositivo elettronico utente (30),
configurati per scambiare dati tra loro, e
in cui il sistema (1) è configurato per implementare il metodo secondo una qualsiasi delle rivendicazioni precedenti.

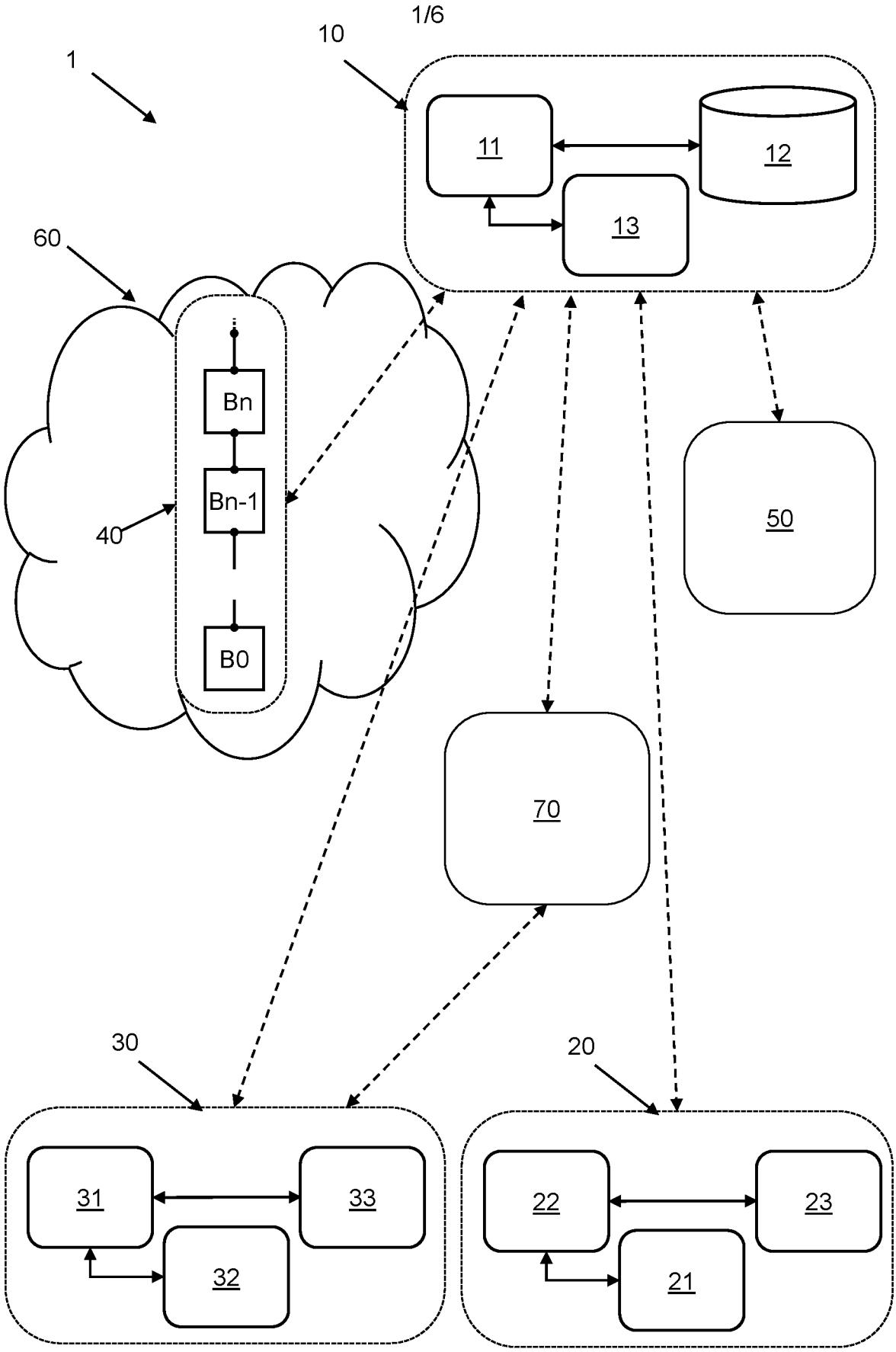


Fig.1

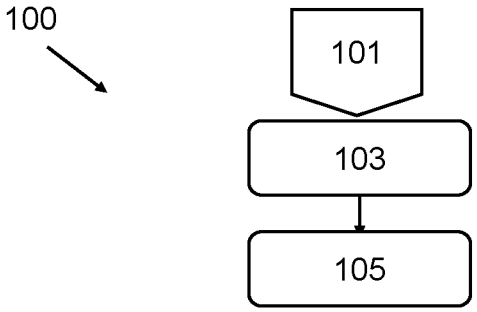


Fig.2

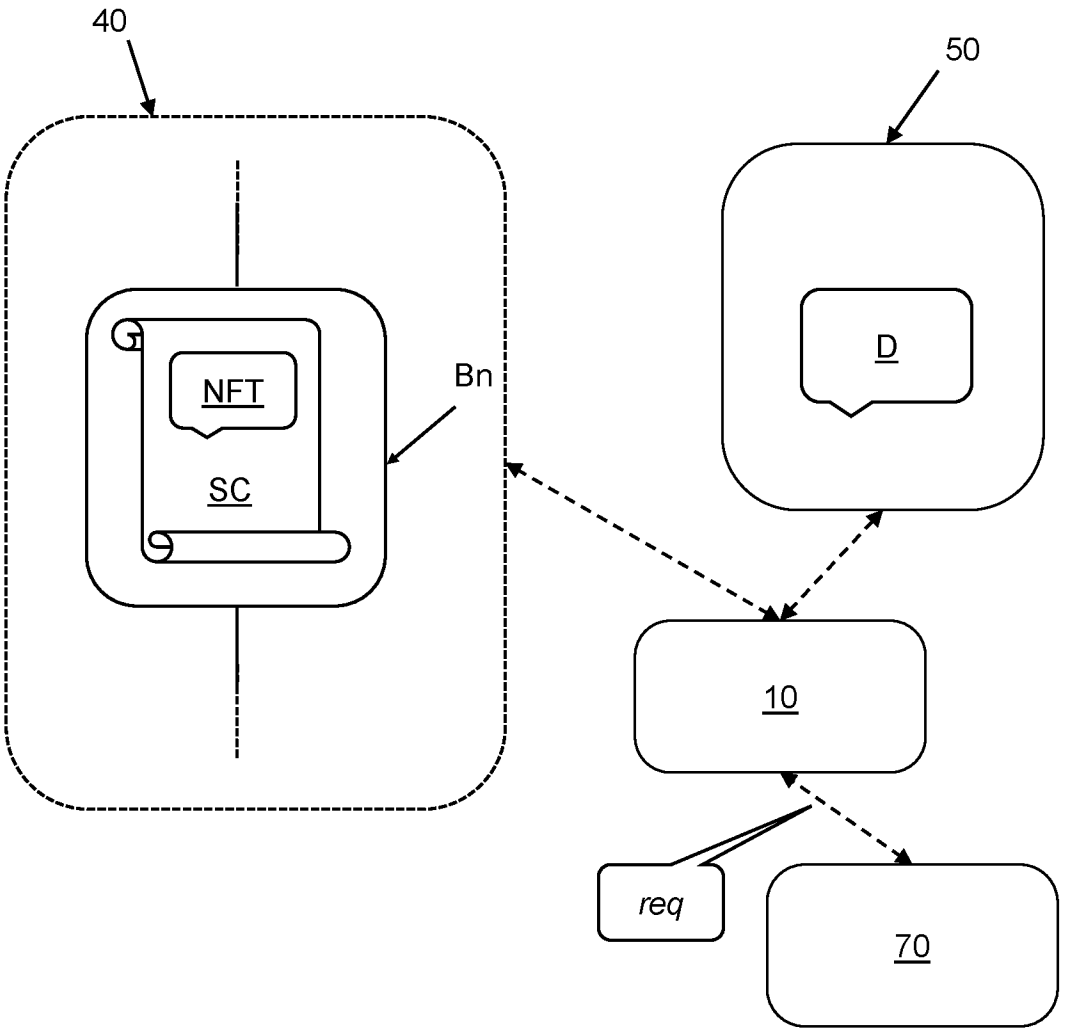


Fig.3

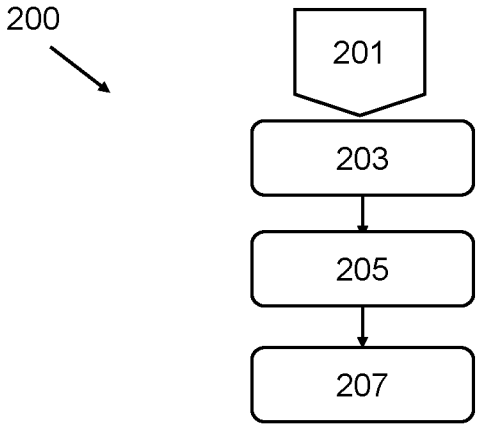


Fig.4

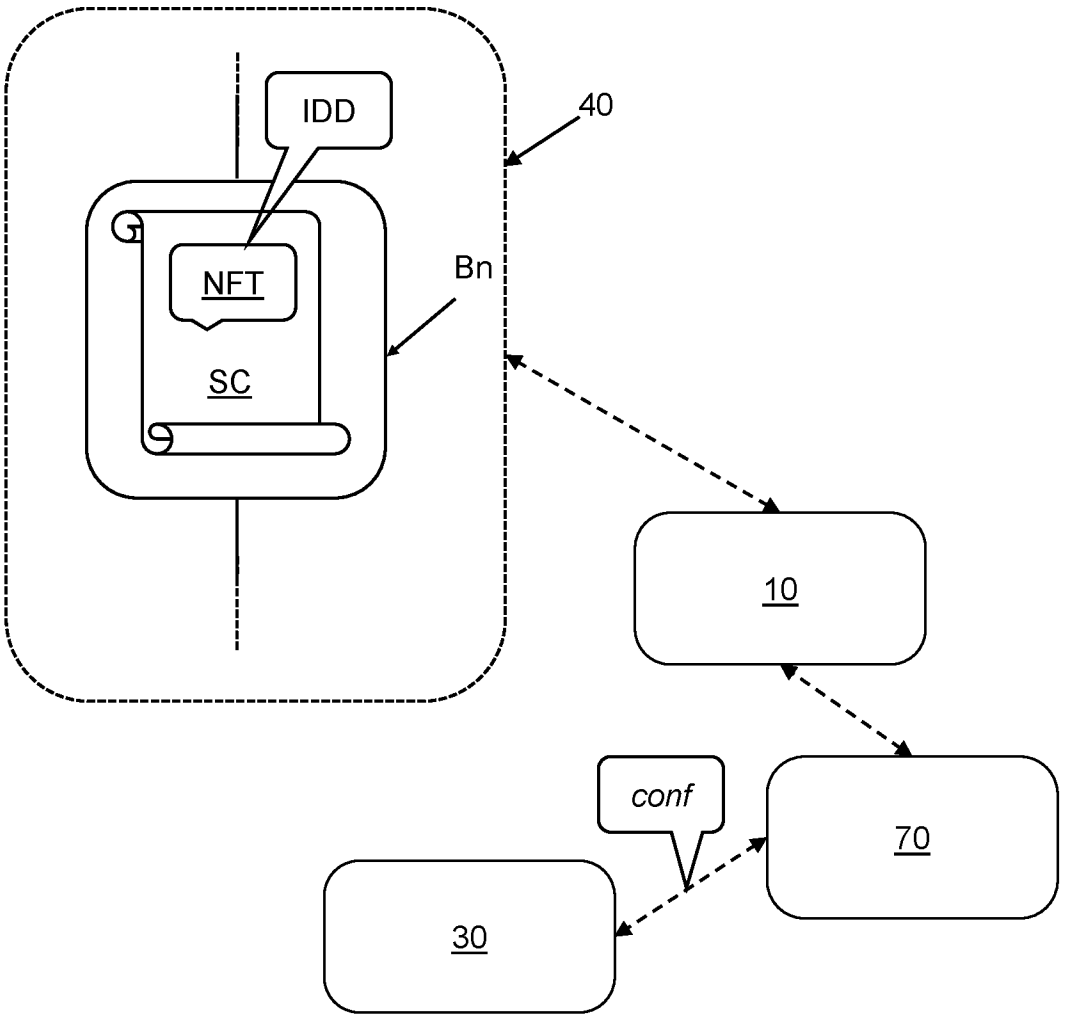


Fig.5

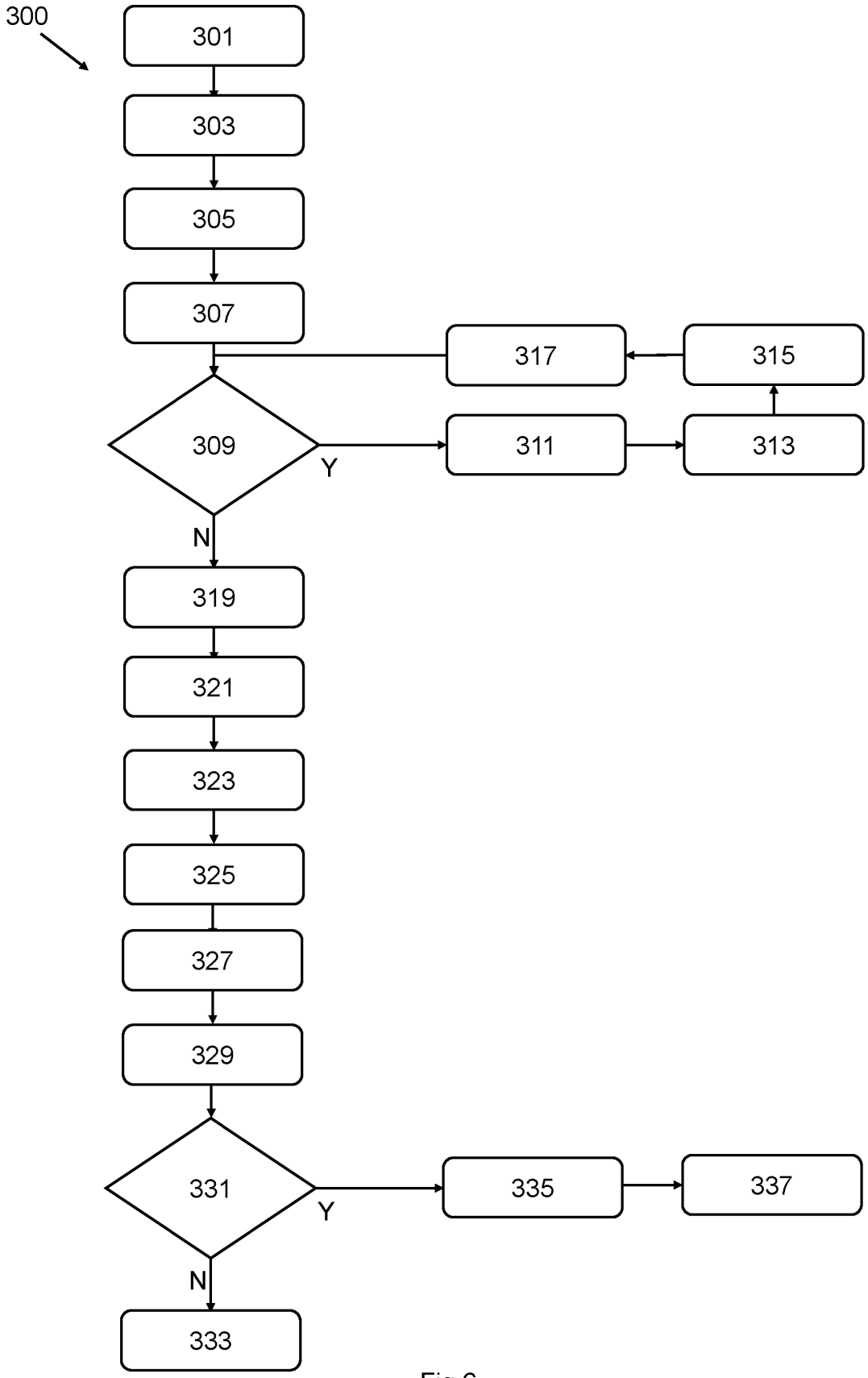
300
301
303
305
307
317
315
309
Y
311
313
N
319
321
323
325
327
329
331
Y
335
337
N
333

Fig.6

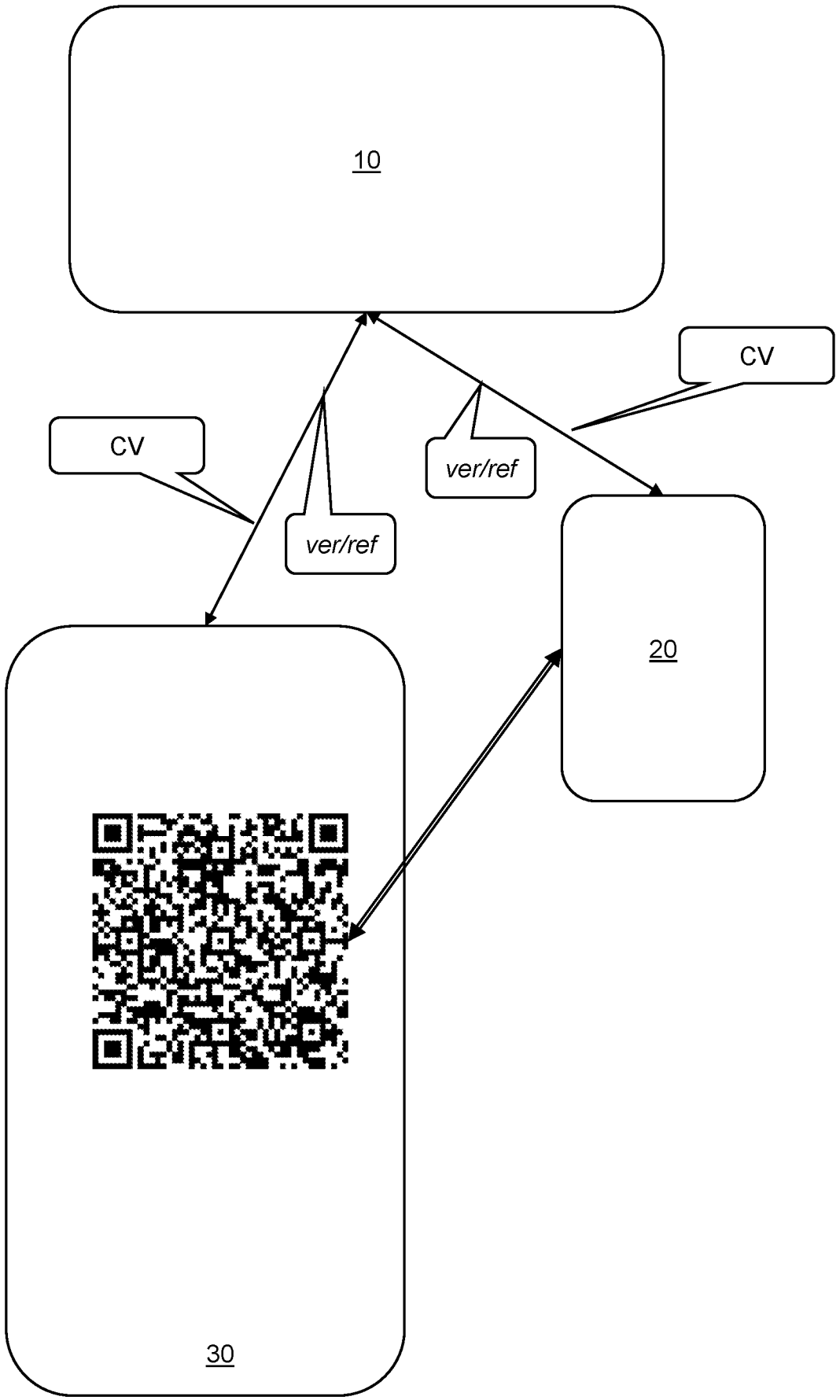


Fig.7

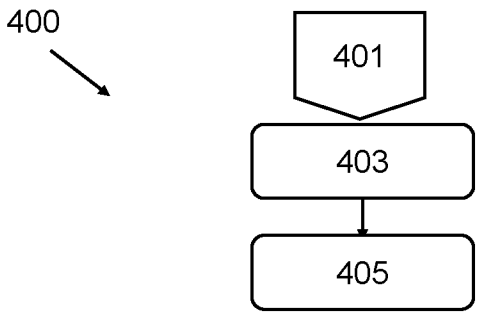


Fig.8